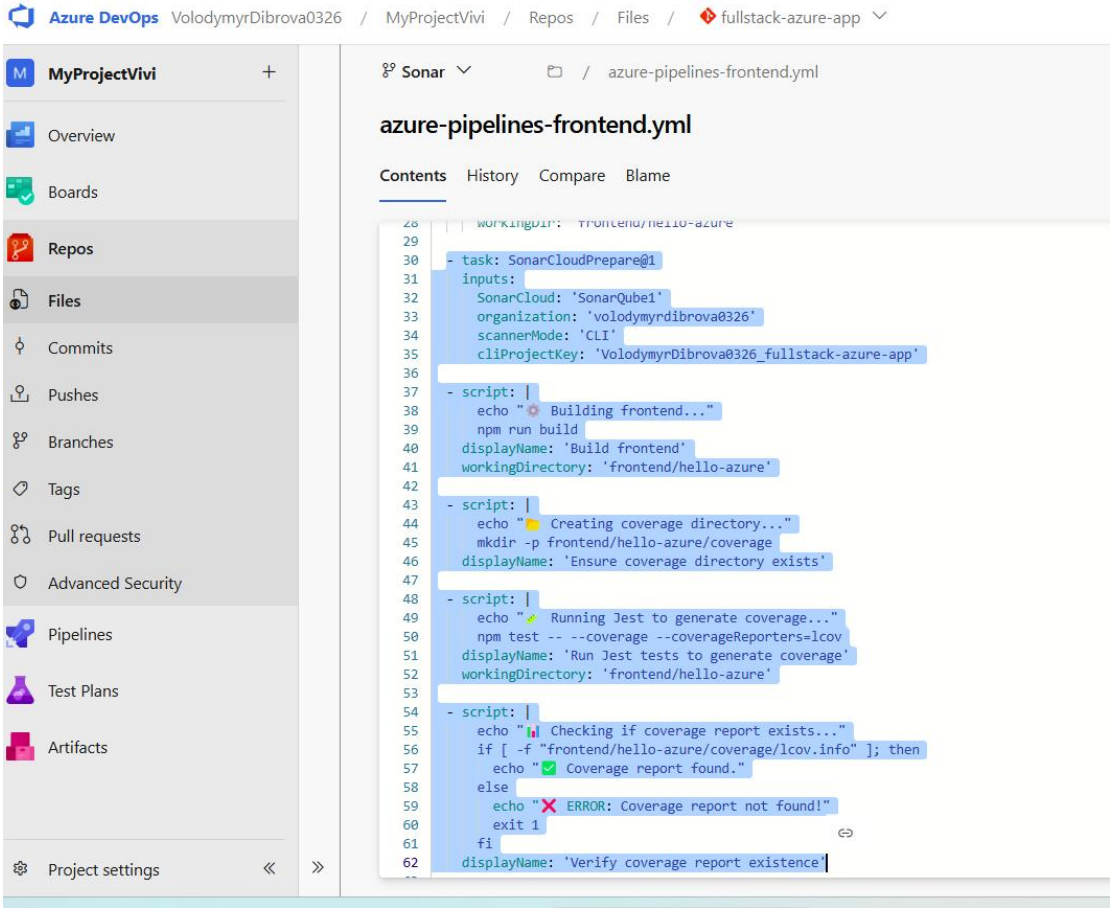
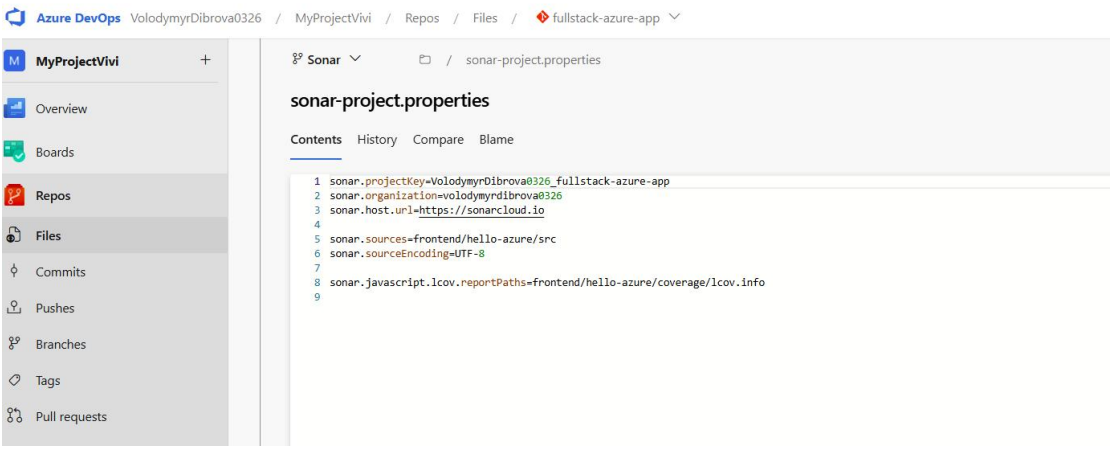
Task 1: Implementing Basic Security Scans in Azure Pipelines

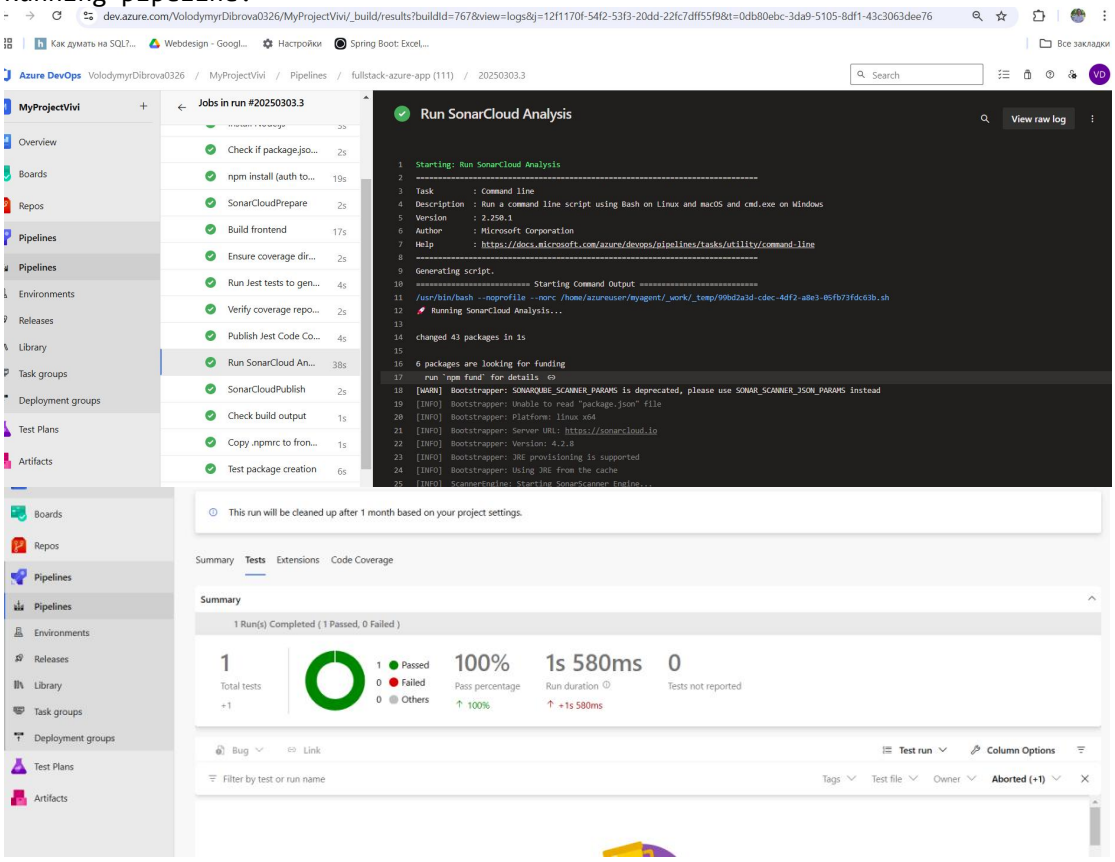
Edited the existing azure-pipeline-frontend file, added SonarCloud



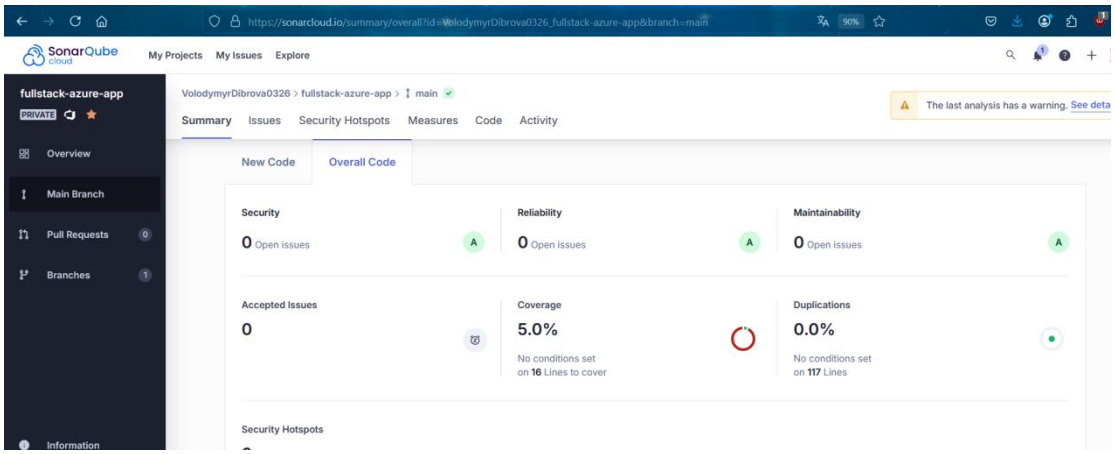
Created sonar-project.properties



Running pipeline:



Result after SonarQube



2.

Task 2: Integrating Azure Security Center with DevOps Workflows

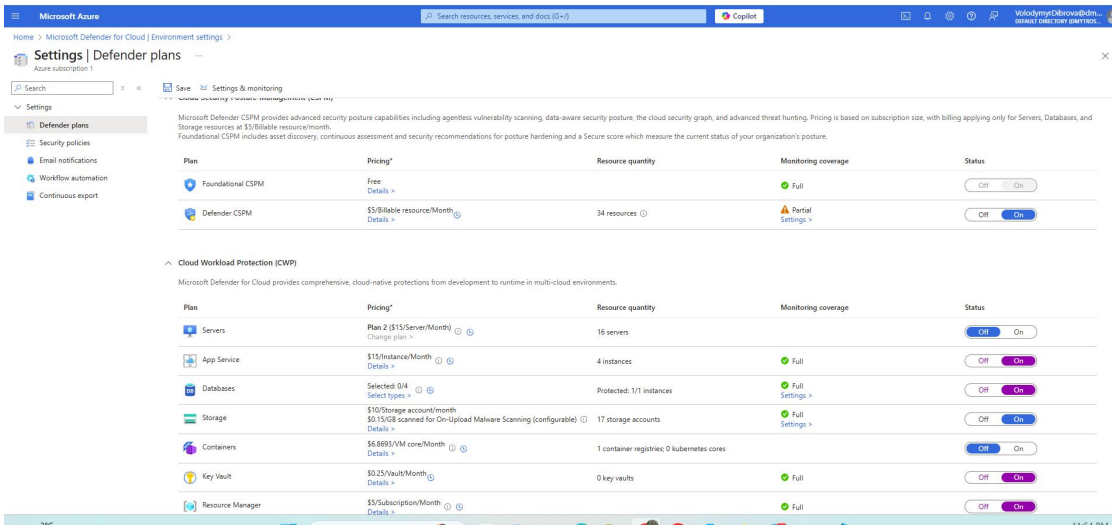
Objective: Configure Azure Security Center to monitor resources and integrate its alerts
into Azure DevOps workflows for automated security incident response.

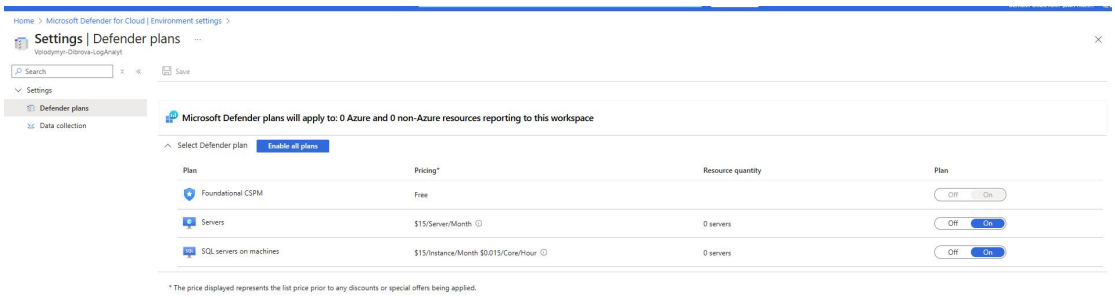
Steps:

- Enable Azure Security Center in your Azure subscription.
- Set up security policies and recommendations for your resources.• Configure alerts for security incidents and integrate them with Azure DevOps using
Azure Logic Apps or Azure Functions.

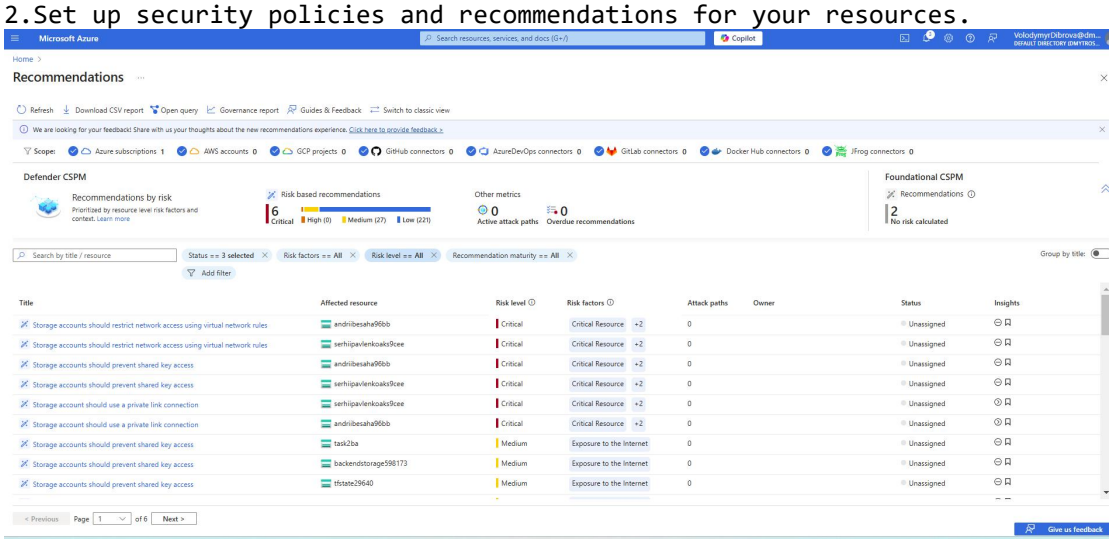
• Create an Azure DevOps work item automatically when a security alert is triggered.
• Test the integration by simulating a security incident and verifying that the workflow
responds appropriately.

1.Enabled Azure Security Center in your Azure subscription.





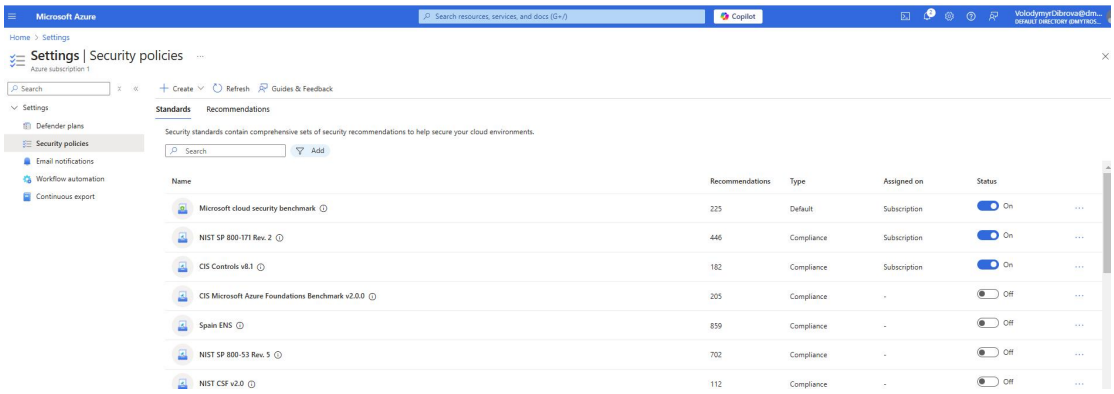
2.Set up security policies and recommendations for your resources.

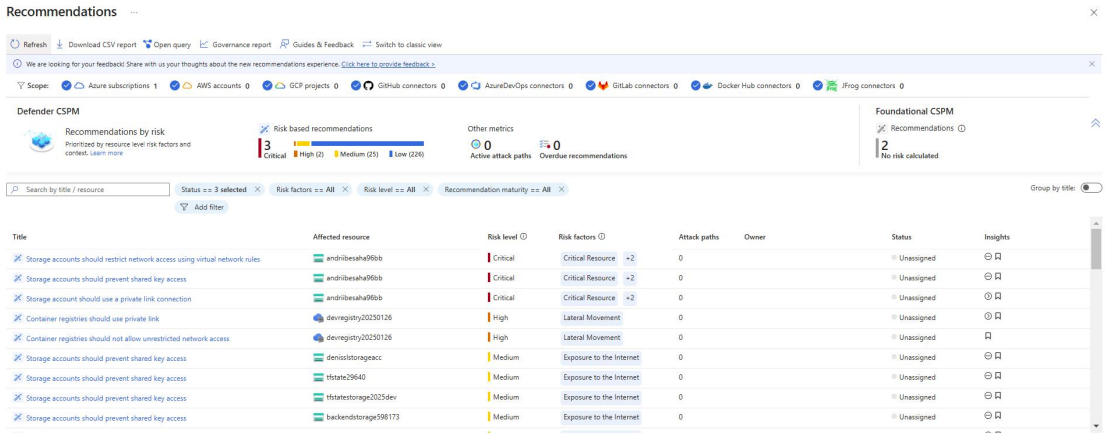


· CIS Microsoft Azure Foundations Benchmark (v2.0.0) – provides advanced security recommendations.

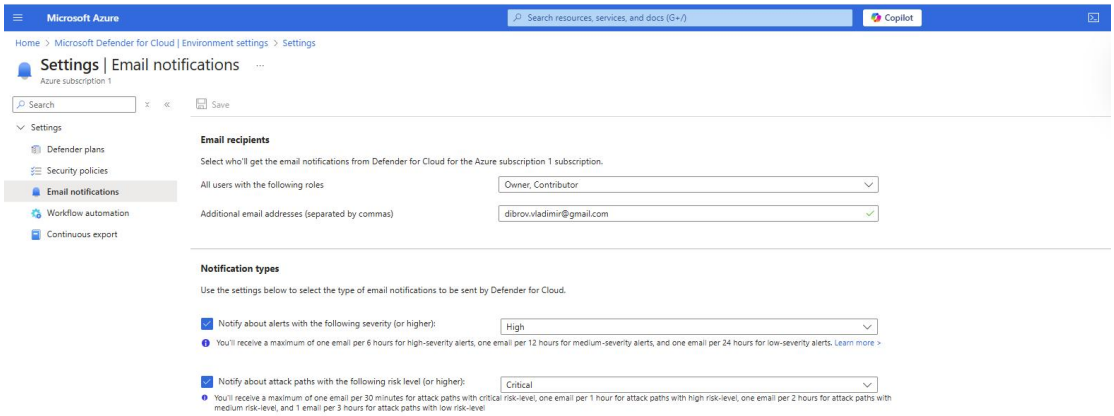
- NIST SP 800-53 Rev. 5 – security standard for regulatory compliance.

- CIS Controls v8.1 – general security practices.

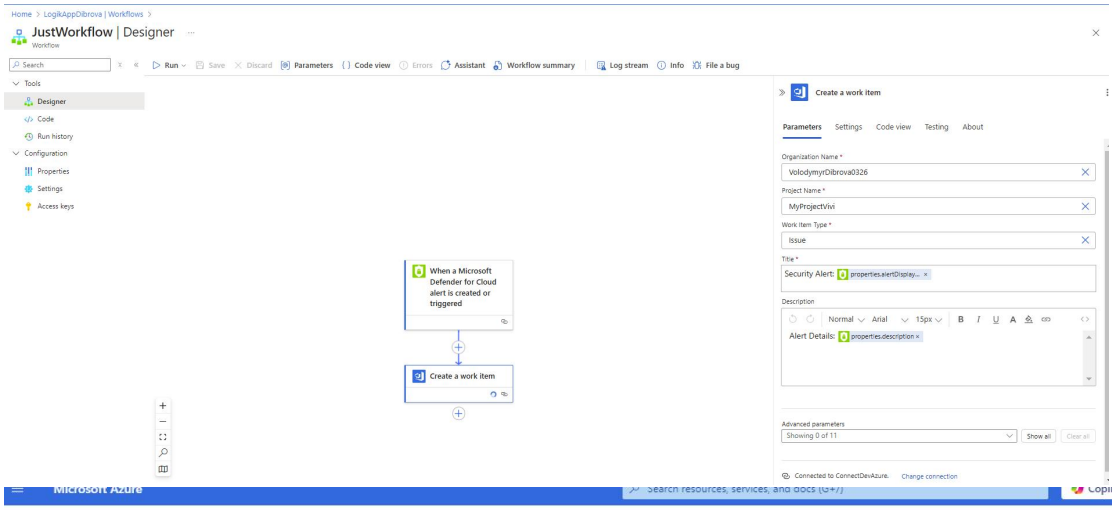


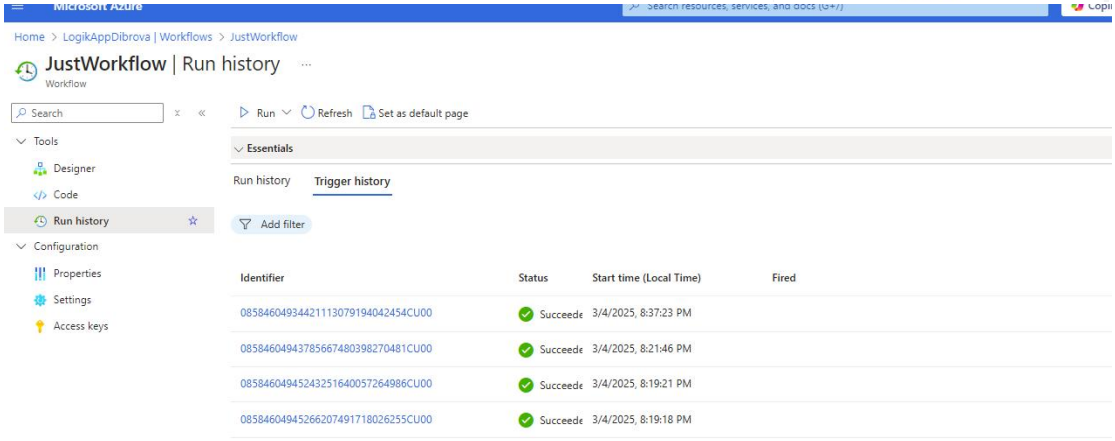


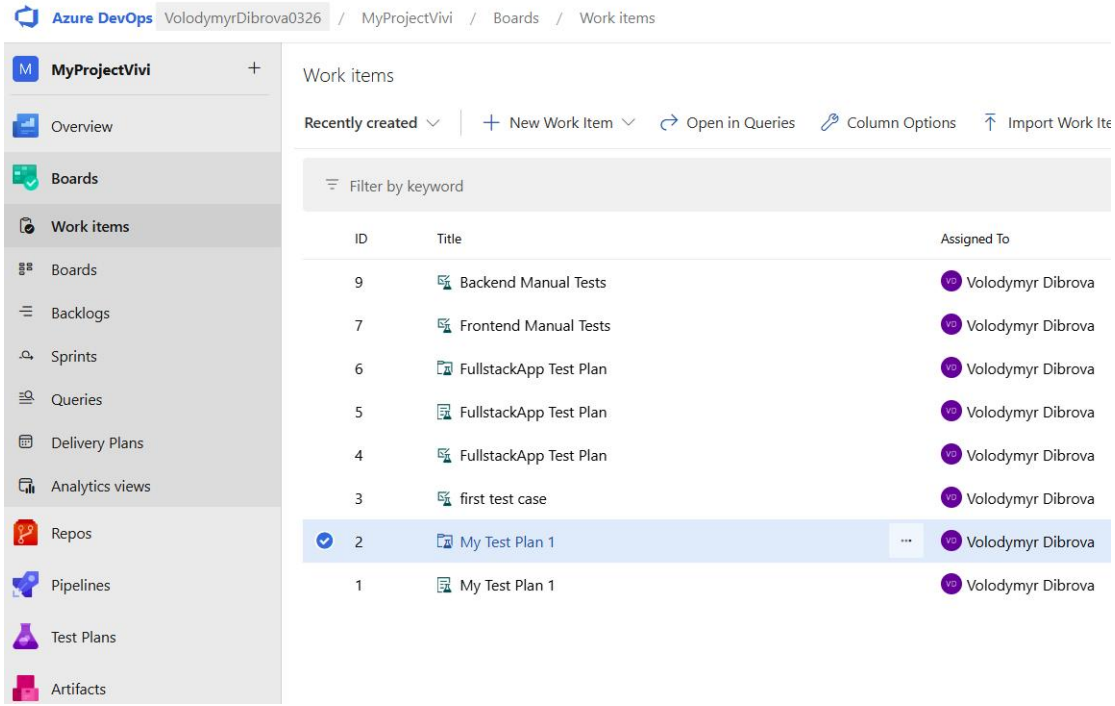
3.Configured alerts for security incidents and integrate them with Azure DevOps using



Azure Logic Apps or Azure Functions.
• Create an Azure DevOps work item automatically when a security alert is triggered.


Home > LogikAppDibrova | Workflows >
JustWorkflow | Designer
Workflow
Run
Save
Discard
Parameters
Code view
Errors
Assistant
Workflow summary
Log stream
Info
File a bug
Tools
Designer
Code
Run history
Configuration
Properties
Settings
Access keys
When a Microsoft Defender for Cloud alert is created or triggered
Create a work item
Create a work item
Parameters
Settings
Code view
Testing
About
Organization Name *
VolodymyrDibrova0326
Project Name *
MyProjectVivi
Work Item Type *
Issue
Title *
Security Alert: properties.alertDisplay...
Description
Normal
Arial
15px
Alert Details: properties.description
Advanced parameters
Showing 0 of 11
Show all
Clear all
Connected to ConnectDevAzure.
Change connection


Home > LogikAppDibrova | Workflows > JustWorkflow
JustWorkflow | Run history
Workflow
Search
Tools
Designer
Code
Run history
Configuration
Properties
Settings
Access keys
Run
Refresh
Set as default page
Essentials
Run history
Trigger history
Add filter
Identifier
Status
Start time (Local Time)
Fired
08584604934421113079194042454CU00
Succeede
3/4/2025, 8:37:23 PM
08584604943785667480398270481CU00
Succeede
3/4/2025, 8:21:46 PM
08584604945243251640057264986CU00
Succeede
3/4/2025, 8:19:21 PM
08584604945266207491718026255CU00
Succeede
3/4/2025, 8:19:18 PM


Azure DevOps
VolodymyrDibrova0326
/
MyProjectVivi
/
Boards
/
Work items
MyProjectVivi
Overview
Boards
Work items
Boards
Backlogs
Sprints
Queries
Delivery Plans
Analytics views
Repos
Pipelines
Test Plans
Artifacts
Work items
Recently created
New Work Item
Open in Queries
Column Options
Import Work Ite
Filter by keyword
ID
Title
Assigned To
9
Backend Manual Tests
Volodymyr Dibrova
7
Frontend Manual Tests
Volodymyr Dibrova
6
FullstackApp Test Plan
Volodymyr Dibrova
5
FullstackApp Test Plan
Volodymyr Dibrova
4
FullstackApp Test Plan
Volodymyr Dibrova
3
first test case
Volodymyr Dibrova
2
My Test Plan 1
Volodymyr Dibrova
1
My Test Plan 1
Volodymyr Dibrova

Task 3: Implementing a Comprehensive DevSecOps Strategy with Azure Policy and Automation

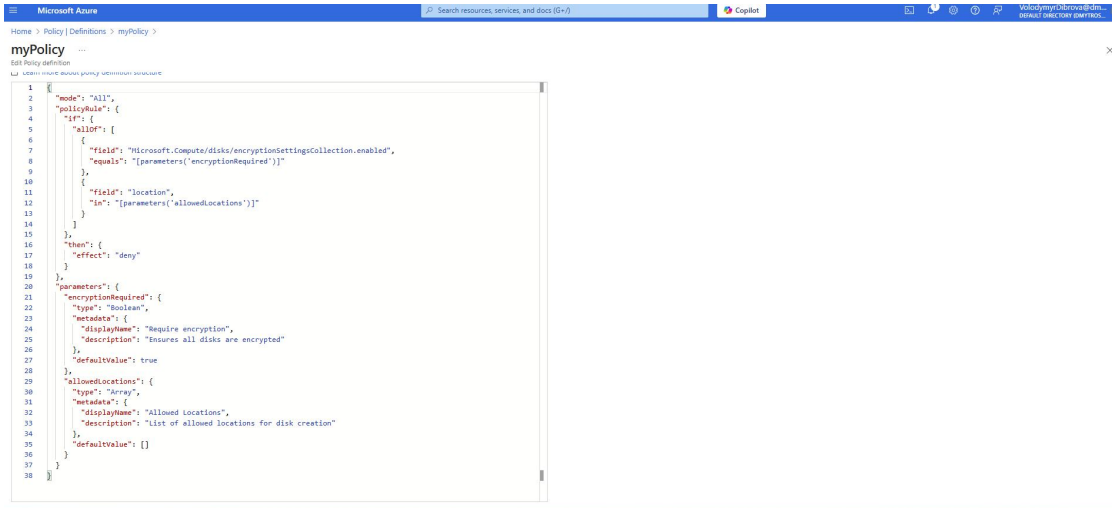
Objective: Implement a comprehensive DevSecOps strategy using Azure Policy, Azure Blueprints, and automation to enforce security best practices, ensure compliance, and streamline governance across your Azure environments.

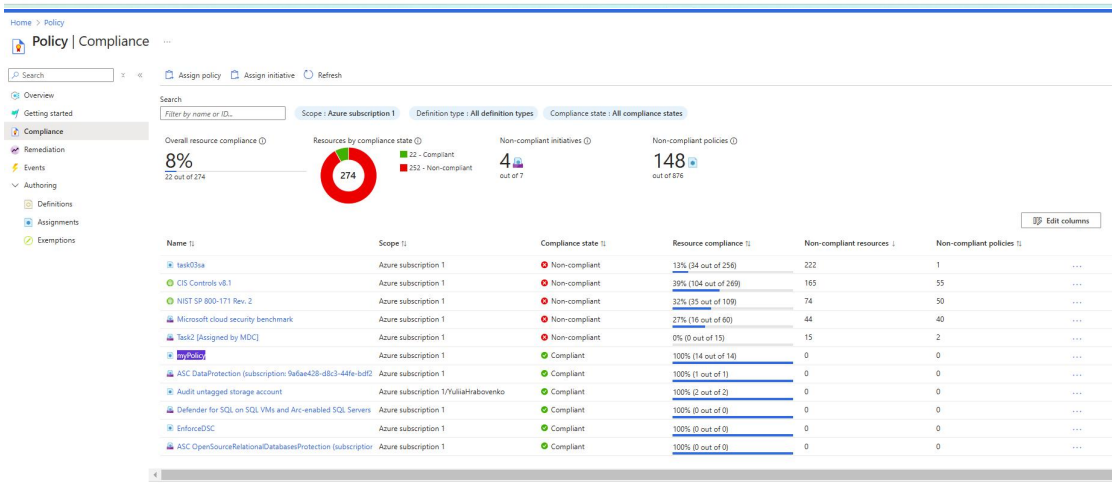
Steps:

- **Create Azure Policies:**
  Navigate to the Azure Portal and go to "Policy." Create or select existing policies that enforce security best practices, such as requiring encryption at rest, ensuring secure network configurations, or enforcing tag usage for resources. Assign these policies to your Azure subscriptions or resource groups to start auditing resources for compliance.
- **Set Up Azure Blueprints:**
  In the Azure Portal, go to "Blueprints." Create a new blueprint definition that includes your Azure Policies, resource templates, and RBAC assignments. Publish and assign the blueprint to your target subscriptions to ensure consistent deployment of resources and policies.
- **Automate Compliance Monitoring:**
  Use Azure Monitor to set up alerts for policy compliance states. Configure Log Analytics to collect and analyze data on policy compliance, creating dashboards to visualize this data.
- **Implement Automated Remediation:**
  Use Azure Automation or Azure Functions to create runbooks or scripts that automatically remediate common policy violations, such as enabling encryption or applying missing tags. Trigger these runbooks based on alerts from Azure Monitor when policy violations are detected.
- **Configure Role-Based Access Control (RBAC):**
  Go to "Access control (IAM)" in the Azure Portal for your resources. Assign roles that adhere to the principle of least privilege, ensuring users have only the permissions they need. Regularly review role assignments and adjust as necessary based on access requirements.
- **Integrate with Azure DevOps:**
  Set up Azure DevOps pipelines to include policy compliance checks using Azure CLI or Azure PowerShell tasks. Use these tasks to ensure that resources deployed through the pipeline are compliant with your defined policies.
- **Test and Validate the Implementation:**
  Deploy a test resource using your blueprint and verify that all policies are applied

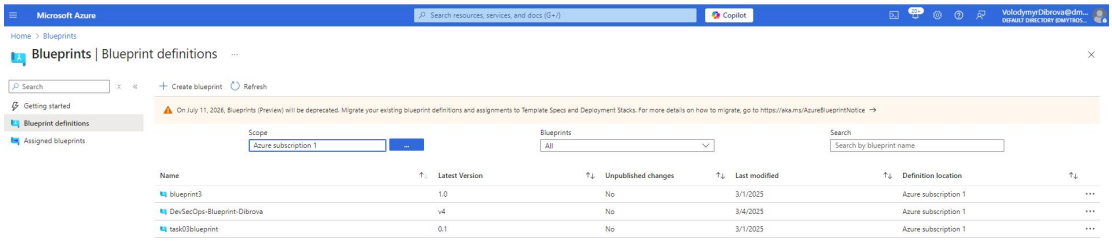
and compliant. Simulate a policy violation and test the automated remediation
process to ensure it works as expected.

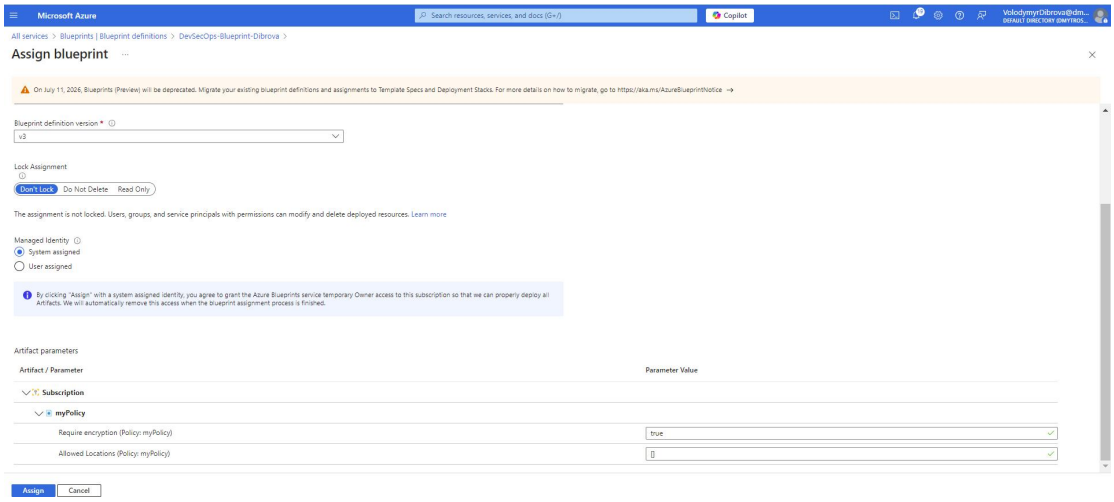
Create Azure Policies and Assigned

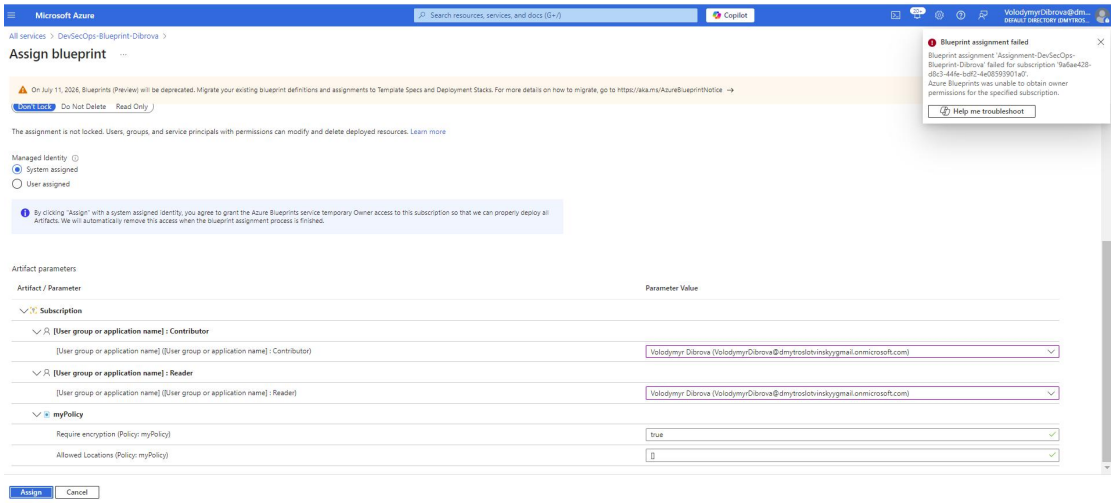




Set Up Azure Blueprints



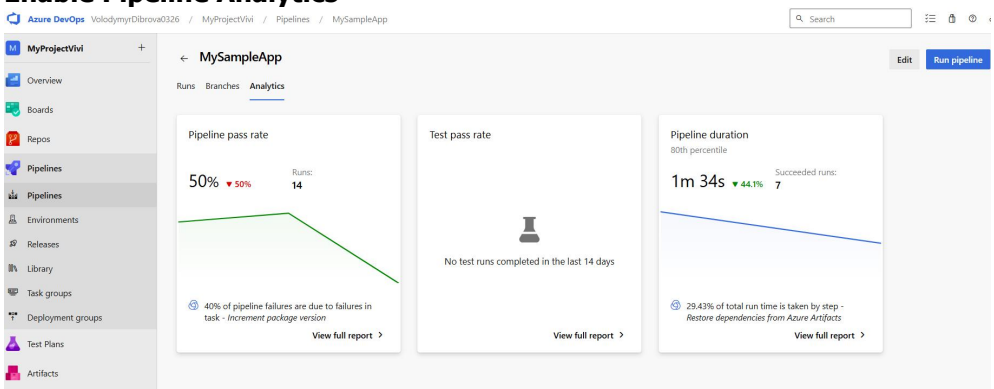


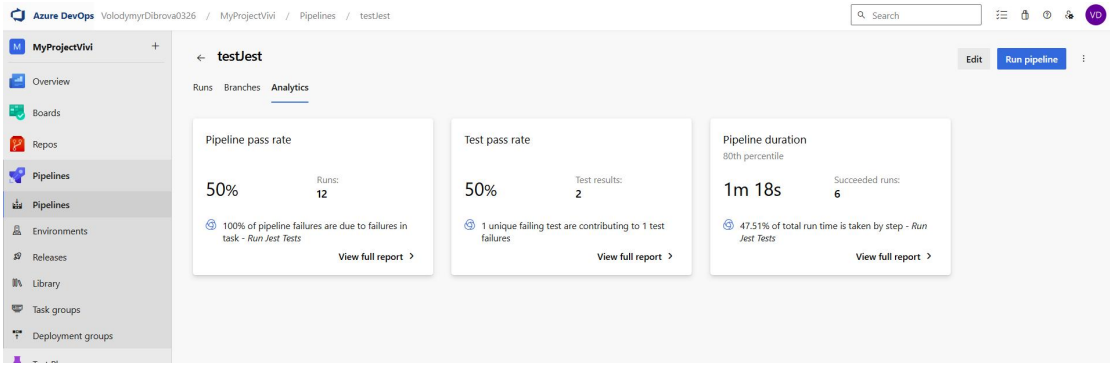


Issue: I cannot continue the task because I don't have Contibutor permissions on the subscription. Azure Blueprints requires Contibutor access to assign policies and deploy resources. Without this permission, the assignment fails.

Task 4: Monitoring DevOps Pipelines for Health and Performance
Objective: Set up a monitoring solution to track the health and performance of your Azure
DevOps pipelines, ensuring timely detection and resolution of issues to maintain efficient CI/CD processes.

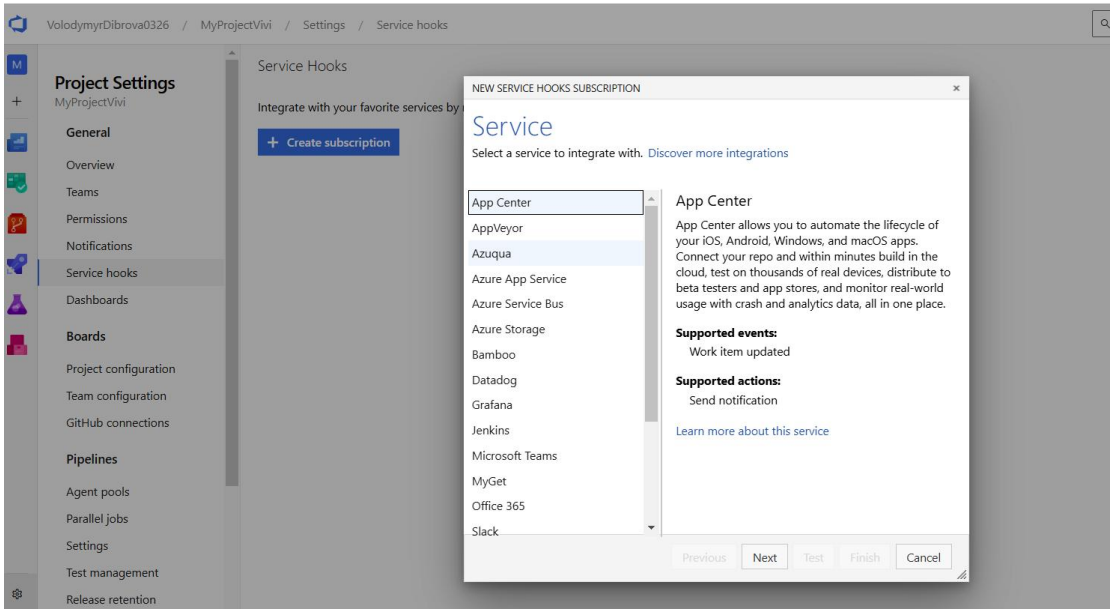
Enable Pipeline Analytics

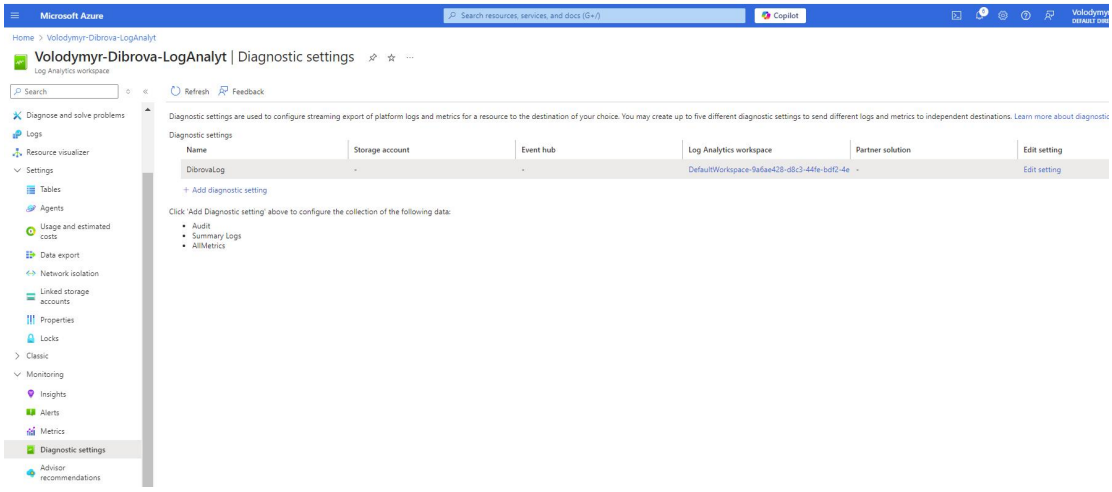




Integrate Azure Monitor for Logs

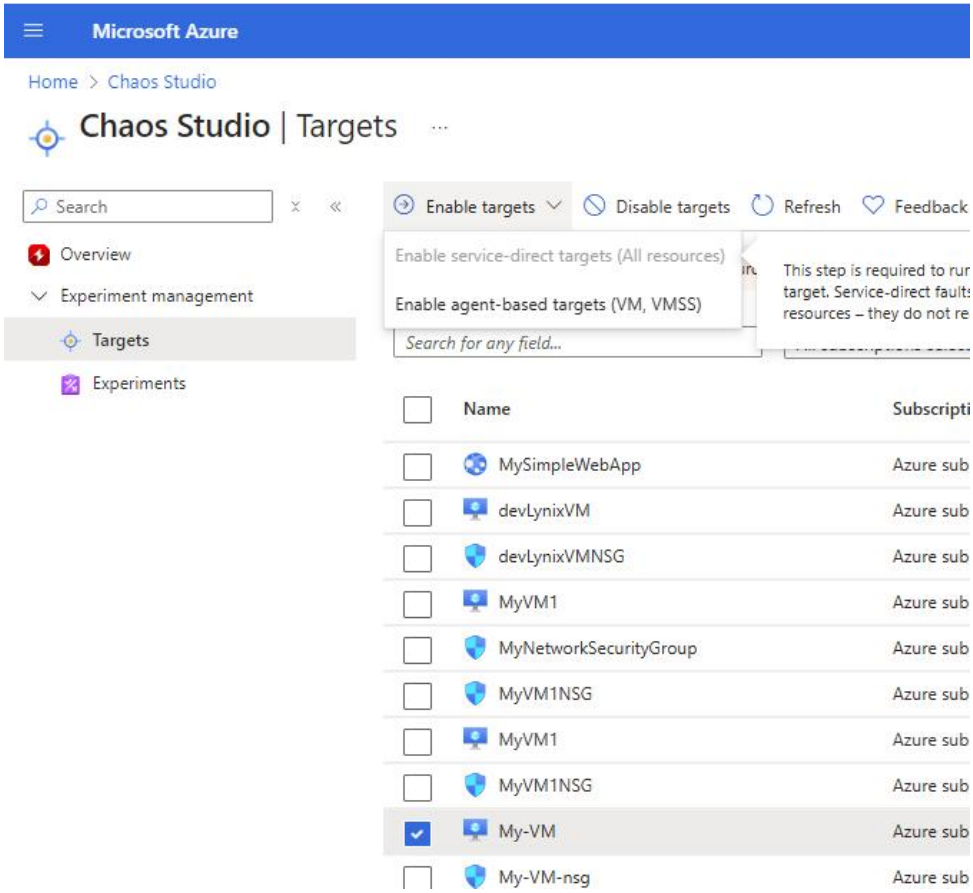
I tried to add a new Azure Monitor (Log Analytics) service to Service Hooks.
Then I would connect to Log Analytics in the Azure portal
But:
This means that the Azure DevOps Services Connector for Azure Monitor is not available, I don’t have the required "Organization Owner" access rights.



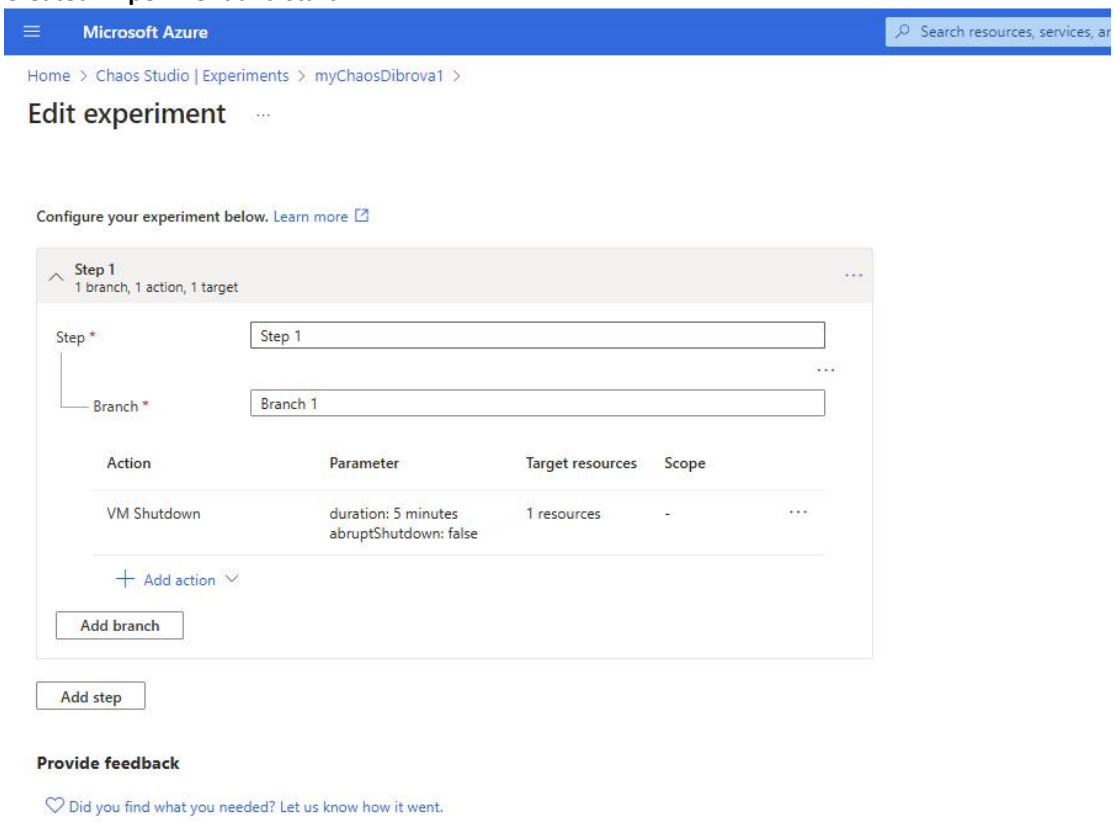


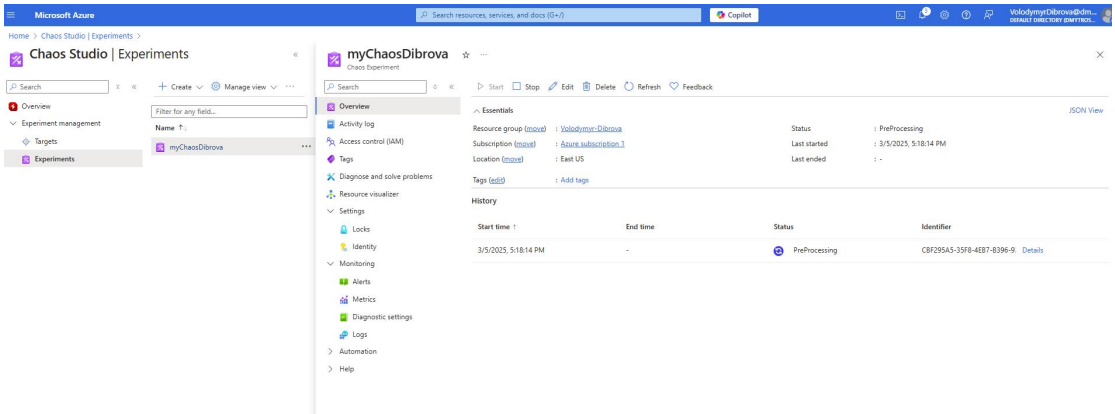
Task 5: Implementing Chaos Engineering in Azure with Azure Chaos Studio
Objective: Use Azure Chaos Studio to conduct chaos experiments on Azure resources, testing the resilience of your applications and infrastructure to improve their reliability and stability.

Enabled target

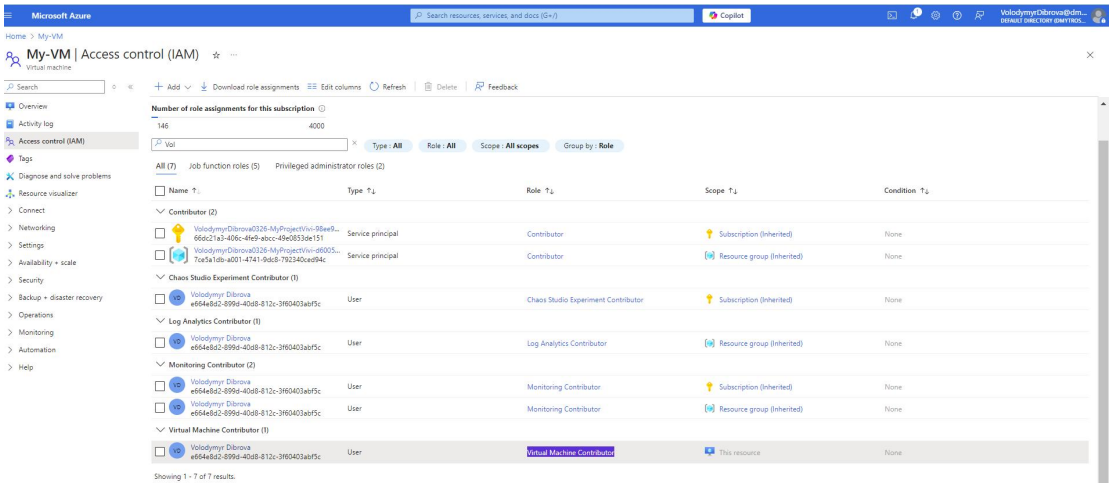


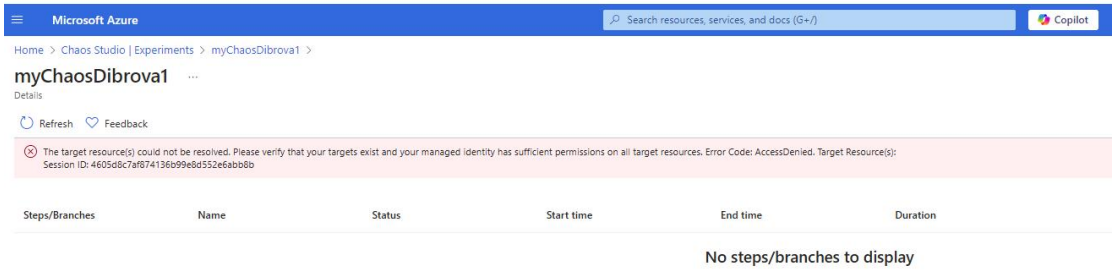
Created Experiment and start





Added access





Issue: I cannot continue the task because I have problem with permissions on the subscription but I'm added.